CREATING THE RESILIENT ORGANIZATION OF THE FUTURE (BUSINESS CONTINUITY)

SHRM VA State Retreat

April 22, 2024

K·N·S Consulting

Presented by Kathy Scourby CBCP, CCRP - KNS Consulting

DEFINITION OF
DISASTER OR CRISIS

"Any situation that threatens the integrity or reputation of a firm or business, usually brought on by adverse or negative media attention."

K·N·S
Consulting

"ORDINARY" CRISIS VULNERABILITY

Fire/Floods/ Bad Weather/ Natural Disasters

Tripledemic Outbreaks (loss of Employees)

Extended Power Outage

Cyber Issues/Data Breach/ Ransomware

Workplace Violence/ Terrorism

Death of Key Individual(s) in Your Firm

K·N·S
Consulting

Reasonable Foreseeability of Disasters

01 It is not a question of “IF”, but “WHEN”

02 Potential Violation of Ethical Rules

03 Potential Professional Negligence Liability

04 Potential loss of Revenue, Reputation & Clients

K·N·S Consulting

Business Continuity
(Operational and Financial Resilience)

K·N·S Consulting

Impacts of "Disasters" to Businesses

Lack of productivity from employers and staff

Supply Chain Interruptions

Delay of Services provided to both Clients/Customers and Firms

Increased Expenses for both Clients/Customers and Firms

Increased risk of data breaches, ransomware and phishing/hacking

Inability to work at home efficiently

Staffing changes in both employer and staff ranks

Hybrid working environment: Leaders and Staff not wanting to return to the office

Harm to Firm Reputation

K·N·S Consulting

Resiliency for the Future – Office vs. Hybrid Work

Continuing to Protect and Care About Your Work Force

- Physical office guidelines and working with building management
- WFH concerns/decisions as to who can continue to work from home and how often
- Space planning with landlord. Do you continue to need space? What about “hoteling” concept?
- Awareness meetings for all leaders and staff dealing with “back in the office” expectations

Resiliency for the Future – Using Technology Tools

- Awareness of the importance and review all IT security policies and technology being used in business
- Technology is more critical to how well organizations meet client/customer expectations (76% understand the need but only 28% are prepared to address)
- 81% of corporate legal departments will require prospective law firms to make sure their technology is more productive and efficient (compared to 41% today) (e-discovery, client/law firm data portals, etc.)

** 2020 Wolters Kluwer survey*

Resiliency for the Future – Business Continuity

- Run business like a well-oiled business with a culture that encourages communication, openness, access and collaboration with clients/customers and all workforce
- Constantly review supply chain issues and implement vendor risk management program (be prepared)
- Plan for the next “downturn” now
- Think about overall risk level and risk tolerance for your organization (what level of risk will you accept?)

Resiliency for the Future –

Guidance for working with Clients/Customers

MANAGING AND WORKING WITH CLIENTS:

- Have a good understanding of client/customer industries
- Continue to offer to meet with clients/customers and listen to their needs. Are they financially sound?
- CROSS SELLING/CROSS TRAINING ACROSS ORGANIZATION
- Renegotiation of fees and the slow paying client/customer. Always be open to alternative fee arrangements.
- Ending a relationship with a client/customer who does not pay
- Start Firm Succession Planning NOW

Business Continuity Planning (Reputational Resilience)

K·N·S Consulting

THE NEED FOR A COMPREHENSIVE
Business Continuity Plan For Any Disaster

01

Compliance issues (Client audits and RFP's)

02

Regulatory Requirements (Government or ISO/NIST certification)

03

New hardware or operating systems and applications that are in the Cloud (cyber/data breach concerns)

04

Facility and/ or personnel changes/moves /relocation (Physical security and vulnerability concerns)

05

Changes in voice/data networks (cyber/data breach concerns)

06

Changes in critical third-party vendors and suppliers (cyber/data breach concerns)

07

Tripledemic Planning

(Employee availability concerns)

K·N·S
Consulting

Essential Components of Business Continuity Plan

1. Risk Management Issues
2. Crisis Communication Systems
3. Business Impact Analysis
4. Disaster Recovery Plan in place for IT
5. Continuity of Business – work location option
6. Business Interruption Insurance Coverage
7. Written Business Continuity Plan
8. Crisis Management & Communications Teams
9. Testing Business Continuity Plans

Risk Management Issues

- **Past Disaster Situations**
- **Geographic Locations**
- **Internal Systems or Processes Failures**
- **Neighbor Disaster:** will your office be affected?

Crisis Communication Systems

(How You Operate/Communicate Becomes Your Own Disaster Plan)

Telephone Tree System

Toll-free emergency # all employees

Automated notification systems (reverse 911)

Password protected web page/ Dashboard

Test, Test, Test update all systems frequently

Using Social Media

K·N·S Consulting

Resiliency for the Future – Business Continuity

Conduct Business Impact Analysis (BIA)

- Determine critical business processes within the organization (every business unit or department)
- Determine key critical/essential personnel and who needs to be in office vs working from home now and in the face of a disaster

Streamline administrative procedures based on results of Business Impact Analysis

Need Plan A, B and C in a Disaster

A

Work remotely from home

B

Work from another office or location

&

Temporary office facilities

C

Contract with disaster recovery provider (mobile units or alternate facilities)

Alternate Workspace Plans

Ultimate goal: providing continuing service to clients

Disaster Recovery For IT

- Ensure networks are backed up consistently and test backups
- Consider moving primary networks off-site and all applications to the Cloud
- Redundancy is important and knowledge of building IT/HVAC systems
- Cyber Security Protection – have intrusion and hacking detection programs in place. Have Data security policies DOCUMENTED and TEST OFTEN!

K·N·S Consulting

Resiliency for the Future – Cybersecurity Awareness

- **Awareness of the importance of cybersecurity issues and security needed within businesses:**
  - Seven (7) law firms were victims of Maze and REvil hackers in 2020)
  - Data stolen included HIPPA consent forms and data from personal injury court cases
  - Lack of compliance with legislation (GDPR, CCPA and HIPPA) can result in severe financial penalties

Use of technology methods including secure firm servers, multi-factor authentication, encryption, EDR, no public Wi-Fi or personal only devices

THE NEED FOR A COMPREHENSIVE CYBER RESILIENCE PLAN

Resilience – An organization must take a holistic approach to understand and prioritize their own entity risk, implement risk management activities, and understand impacts for their own entity as well as those customers/clients to whom they provide services.

- Cyber incidents disrupt an organization's ability to continue to serve customers, meet regulatory requirements and continue to maintain customer confidence.

- Cyber incidents disrupt value creation by eroding public confidence and customer goodwill when personal information is disclosed.

- Understanding and identifying core processes and gaps in cyber resilience plans is critical. Gaps should be eliminated in order to promote cyber resilient processes.

- IT must move from a policing mindset to one that promotes an integrated, comprehensive cyber strategy, powered by people, processes, and technology to support cyber resilience cultural change

TRUST BUT VERIFY

K·N·S Consulting

LONG BEFORE THE DAY YOU GET HACKED

- **Ensure critical organization documents are in the cloud and stored where they are easily accessible**
- **Most recent Air-Gapped Backup and Server image are stored in separate storage locations**
- **All Admin/IT passcodes/hints are in a private cloud account, accessible via smartphones.**
- **Emergency payroll plans and paper checks available if payroll needs to be handled manually**
- **Formal training** on information security/**Information Security reference cards** should be distributed to all users
- **Written internal Cyber Resilience plan** for data security should be part of Business Continuity Plan

K·N·S
Consulting

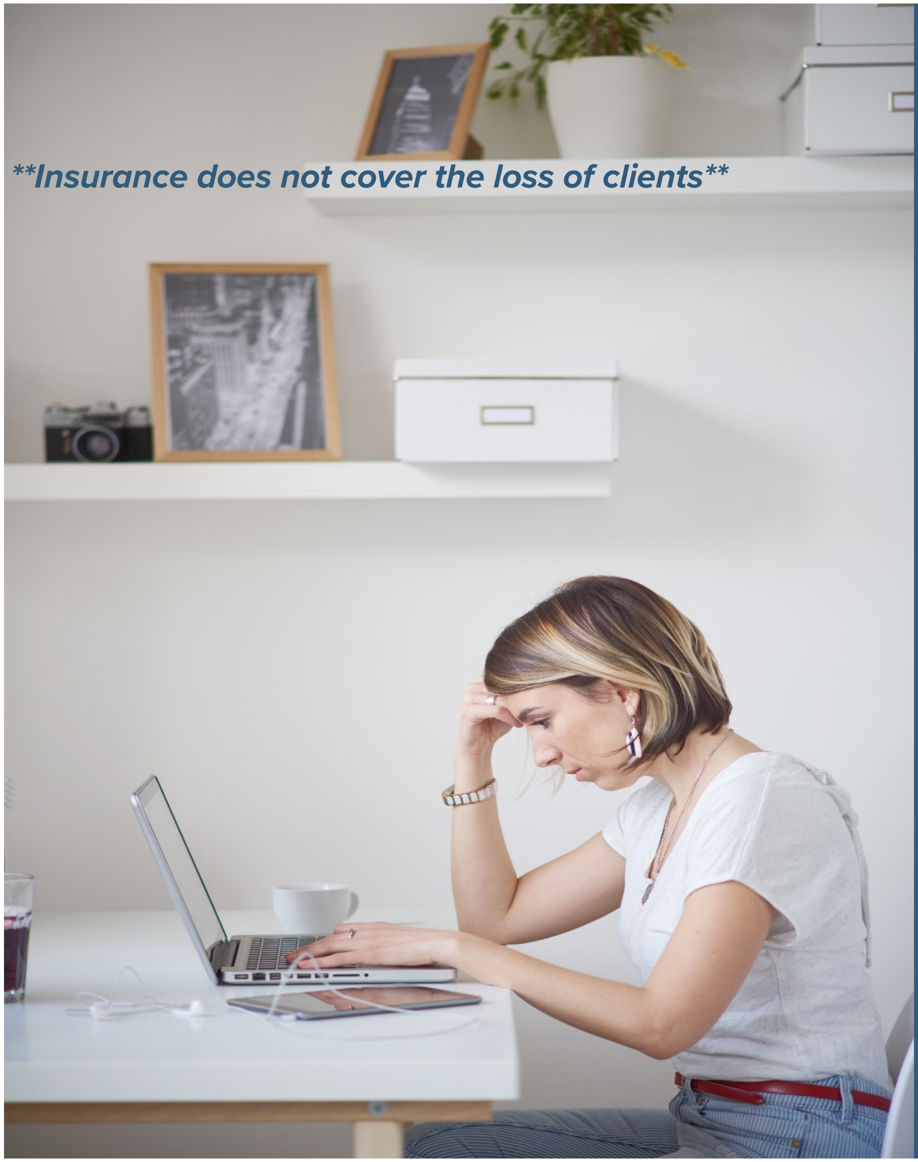
ASSESS VULNERABILITY OF YOUR DATA

- **Perform a Risk Assessment using NIST/ISO or other relevant standards**
- **Conduct independent vulnerability scans of your servers and workstations** at least monthly
- **Verify that software patches are current and applied** in a timely manner every month.
- **Force a restore of some random data set or file/folders** once a week.
- **Conduct a cyber audit** of your cyber insurance coverage
- **Have an understanding of Artificial Intelligence** and its benefits/vulnerabilities for your organization.

K·N·S Consulting

Business Interruption and Cyber Insurance

- Ensure organization has enough coverage if loss to physical property
- Determine how to calculate losses/extra expenses incurred
- Elimination period before coverage kicks in? Exclusions? (Pandemic exclusions?)
- Understand your Cyber Insurance policy (Cyber audit)
- Most policies exclude Pandemics and certain cyber issues



Insurance does not cover the loss of clients

VENDOR/BUSINESS PARTNER
RISK MANAGEMENT PROGRAM

Considerations for a Vendor/Business Partner Risk Management Program

- **How well are your cloud-based applications protected** by your vendor and their partners/vendors?
- **How would your company be impacted if your vendor's IT systems** are down for a period of time?
- **Could your vendor's behavior or lack of security** affect your company's reputation?
- **Does your vendor have access** to your organization's intellectual property or clients' data?

K·N·S
Consulting

Written BC Plan

- Well organized and easily communicated
- Contact information for all leaders and staff
- Vendor/business partner contact information
- Checklist format *(easy to use under stress)*
- Store written plan in easily accessible location
- Links to other critical information
- Always keep a written hard copy version
- Consider electronic version/app on phone

TRAINING/EDUCATION/AWARENESS

Consistent training for all employees and crisis team members (if you have a crisis team) is essential

Face-to-Face/ On-Line Training

Webinars

Actual Drills

Table-Top Exercises

Meetings

Phishing, Data breach & Malware Simulations

Exercises

ADVANTAGES AND ADVERSITIES OF ARTIFICIAL INTELLIGENCE

FOCUS ON AI FROM A RISK AND RESILIENCE PERSPECTIVE:

✓ **Benefits of Artificial Intelligence**

✓ **Misinformation**

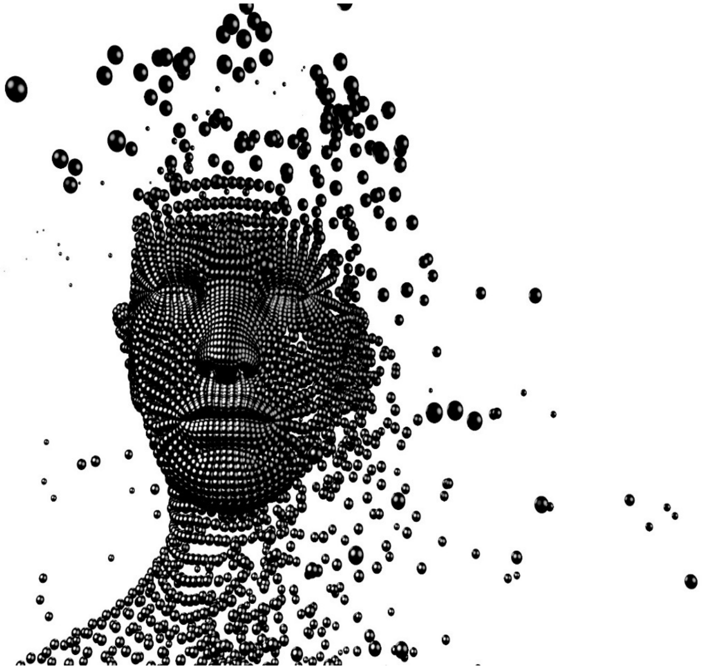
✓ **Deep Fakes**

✓ **Inadvertent Biases**

✓ **Ethical Considerations**

✓ **Evolving Regulatory Landscape**

- **EU - DORA**
- **Biden's Executive Order**



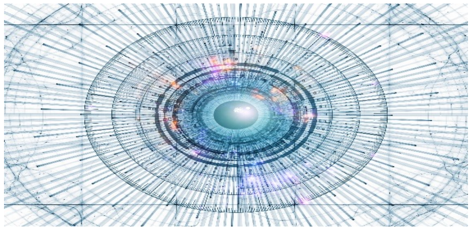
It is all about awareness and education

K·N·S Consulting

ADVANTAGES AND ADVERSITIES OF ARTIFICIAL INTELLIGENCE

FUTURE TRENDS:

1. **CYBERSECURITY is a top priority in all industries (75 – 82% of industry and technology audit leaders)**
2. **ARTIFICIAL INTELLIGENCE is currently an emerging risk with some significant gaps in organizational preparedness and internal audit proficiency**
3. **GROWING concern in the talent needed to understand the benefits and risks of Artificial Intelligence**



K·N·S Consulting

KEYS TO SUCCESS AND BUSINESS RESILIENCE

- ➢ Leadership within the organization (Succession Planning)
- ➢ Communication, Flexibility, Transparency and pivot as necessary
- ➢ Preserve company culture and reputation
- ➢ Be known as a caring organization
- ➢ Conduct Business Impact Analysis
- ➢ Have a written Business Continuity Plan
- ➢ Ensure Data security at the highest level
- ➢ Plan ahead and be ready for the next Disaster

Kathy Scourby, CBCP, CCRP
KNS Consulting, LLC
(865) 789-7694
kscourby@knsbusinessconsulting.com
www.knsbusinessconsulting.com

K·N·S
Consulting